UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/995,308	11/27/2001	Paul Ducharme	VIXS.0100300	9477

29331 7590 01/24/2006

TOLER & LARSON & ABEL, L.L.P.
5000 PLAZA ON THE LAKE
SUITE 265
AUSTIN, TX 78746

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/995,308	DUCHARME, PAUL	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-14,17-22 and 24-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9, 11-14, 17-22, and 24-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/22/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-9, 11-14, 17-22, and 24-41 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-6, 8-10, 13, 14, 33-36, and 41 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Easter et al. U.S. Pat. No. 5563950 (hereinafter Easter) in view of Van Oorschot et al. U.S. Pat. No. 5850443 (hereinafter Van Oorschot).

4. As per claim 1, Easter discloses monolithic semiconductor device comprising: a memory location having an output port coupled to the input port, wherein a data value to be stored in said memory location is observable only internally to the monolithic semiconductor device (Easter: figure 2 and column 4 lines 49-65 and column 2 lines 62-64); an asymmetrical encryption engine having an input port coupled to the output port of the memory location and an output port to provide a symmetrical encryption key based on the data value (Easter: figure 5 and column 8 lines 18-26); and a symmetrical encryption engine having an input port coupled to an output port of the asymmetrical encryption engine, wherein the symmetrical encryption engine is to perform an encryption function using the symmetrical encryption key (Easter: figure 5 and column 8 lines 18-26). In addition, Van Oorschot discloses that the asymmetrical encryption key is

output to symmetrical encryption engine (Van Oorschot: column 5 lines 39-59). It would have been obvious to one having ordinary skill in the art to allow one encryption engine to provide key information to the other encryption engine either directly or indirectly. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Van Oorschot within the system of Easter because it provides multiple layers of encryption/decryption to secure data being transferred.

5. As per claim 2, Easter discloses the monolithic semiconductor device as in claim 1. Easter further discloses wherein said memory location is observable only to said asymmetrical encryption engine (Easter: figure 5 and column 4 lines 50-65 and column 5 lines 26-35: the fuse array).

6. As per claim 3, Easter discloses the monolithic semiconductor device as in claim 1. Easter further discloses said memory location is to store an encryption key (Easter: figure 2 and 5 and column 4 line 57 – column 5 line 11).

7. As per claim 4, Easter discloses the monolithic semiconductor device as in claim 1. Easter further discloses wherein said memory location includes a register (Easter: figure 2).

8. As per claim 5, Easter discloses the monolithic semiconductor device as in claim 1. Easter further discloses wherein said memory location includes non-volatile memory (Easter: column 4 lines 57-65).

9. As per claim 6, Easter discloses the monolithic semiconductor device as in claim 5. Easter further discloses wherein a value stored in said memory location is defined during a manufacture of the monolithic semiconductor device (Easter: column 3 lines 54-64).

10. As per claim 8, Easter discloses the monolithic semiconductor device as in claim 6. Easter further discloses wherein the value is defined using a laser etching technique (Easter: column 6 lines 5-13).

11. As per claim 9, Easter discloses the monolithic semiconductor device as in claim 1. Easter further discloses wherein said memory location includes volatile memory (Easter: column 4 lines 57-65).

12. As per claim 10, Easter discloses the monolithic semiconductor device as in claim 9. Easter further discloses wherein a value stored in said memory location is provided by said first encryption engine (Easter: figure 2 and column 4 lines 54-56).

13. As per claim 13, Easter discloses the monolithic semiconductor device as in claim 1. Easter further discloses the device comprising: at least one silicon die pad having an

input coupled to the output of said memory location to provide a temporary access to said memory location (Easter: figure 2 and column 4 lines 50-65).

14. As per claim 14, Easter discloses the monolithic semiconductor device as in claim 1. Easter further discloses the device comprising an unique ID register coupled to the input of said encryption engine to store an unique ID (Easter: column 5 lines 27-36 and figure 3).

15. As per claim 33, Easter discloses a method comprising the steps of: accessing, by a first encryption engine internal to a monolithic semiconductor device, data from a memory location internal to the monolithic semiconductor device, wherein the memory location is accessible only internal to the monolithic semiconductor device (Easter: figure 5 and column 8 lines 18-26); generating, at the first encryption engine, a first encryption key based on the data from the memory location; providing the first encryption key to a second encryption engine internal to the monolithic semiconductor device (Easter: figure 5 and column 8 lines 18-26); and performing an encryption function at the second encryption engine using the first encryption key (Easter: figure 2 and column 4 lines 49-65 and column 2 lines 62-64). In addition, Van Oorschot discloses that the asymmetrical encryption key is output to symmetrical encryption engine (Van Oorschot: column 5 lines 39-59). It would have been obvious to one having ordinary skill in the art to allow one encryption engine to provide key information to the other encryption engine either directly or indirectly. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Van Oorschot

within the system of Easter because it provides multiple layers of encryption/decryption to secure data being transferred.

16. As per claim 34, Easter discloses the method as in claim 33. Easter further discloses wherein the data is accessible only by the first encryption engine (Easter: figure 5 and column 5 lines 24-36).

17. As per claim 35, Easter discloses the method as in claim 33. Easter further discloses wherein the data represents a second encryption key (Easter: figure 5 and column 5 lines 24-36).

18. As per claim 36, Easter discloses the method as in claim 35. Easter further discloses the method including the steps of: generating the first encryption key; and providing the first encryption key for storage in the memory location (Easter: figure 5 and column 8 lines 18-26).

19. As per claim 41, claim 41 encompasses the same scope as claim 13. Therefore, claim 41 is rejected based on the same reason as in claim 13.

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

> the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Easter in view of Loh et al. U.S. Pub. No. 20030093661 (hereinafter Loh).

22. As per claim 7, Easter discloses the monolithic semiconductor device as in claim 6. Easter does not explicitly disclose wherein the value is defined using a lithographic technique. However, Loh discloses that limitation (Loh: [0003]:use of lithography). It would have been obvious to one having ordinary skill in the art to define value of the memory location using lithographic technique because lithography is one of the most common technique for hardwired programming of the ROM on semiconductor. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Loh within the system of Easter because lithography is well known technique in semiconductor industry.

23. Claims 11, 12, 17-19, 21, 22, 24-29, 30-32, and 37-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Easter in view of Van Oorschot and further in view of Pitts U.S. Pub. No. 20020145931 (hereinafter Pitts).

24. As per claim 11, Easter discloses the monolithic semiconductor device as in claim 1. Easter further discloses the device comprising: an external port having an input and output (Easter: figure 2). Easter does not explicitly disclose an isolation portion coupled to the input of said external port and to the output of said memory location, wherein said

isolation portion to prevent access to said memory location using said external port. However, Pitts discloses an isolation fuse element that enforces one time programming of the memory (Pitts: [0011]: the fuse element and figure 1:104). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to include a fuse element in the semiconductor device because semiconductor device with fuse is well known in the art. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Pitts within the system of Easter because it prevents external access to the memory location after data has been successfully stored into secure memory array.

25. As per claim 12, Easter as modified discloses the monolithic semiconductor device as in claim 11. Easter as modified further discloses wherein said isolation portion includes a fuse coupled between the input of said external port and the output port of said memory location (Pitts: [0011]: the fuse element and figure 1:104).

26. As per claim 17, Easter discloses a monolithic semiconductor device comprising: an external data port having an input and an output; a first encryption engine having an input coupled to the input of said external data port and an output (Easter: figure 5 and column 8 lines 18-26); and a second encryption engine having an input coupled to the input of said external data port and an output (Easter: figure 5 and column 8 lines 18-26); a memory location having an output coupled to the input of said first encryption engine (Easter: figure 5 and column 8 lines 18-26); and wherein the first encryption engine is to provide a first encryption key based on a value stored at said memory location to said

second encryption engine (Easter: figure 5 and column 8 lines 18-26). In addition, Van Oorschot discloses that the asymmetrical encryption key is output to symmetrical encryption engine (Van Oorschot: column 5 lines 39-59). It would have been obvious to one having ordinary skill in the art to allow one encryption engine to provide key information to the other encryption engine either directly or indirectly. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Van Oorschot within the system of Easter because it provides multiple layers of encryption/decryption to secure data being transferred. Easter as modified does not explicitly disclose an isolation portion coupled to the output of said memory location and to the input of said external data port, wherein said isolation portion is modifiable to permanently prevent access of said memory location by the external data port. However, Pitts discloses an isolation fuse element that enforces one time programming of the memory (Pitts: [0011]: the fuse element and figure 1:104). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to include a fuse element in the semiconductor device because semiconductor device with fuse is well known in the art. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Pitts within the system of Easter because it prevents external access to the memory location after data has been successfully stored into secure memory array.

27. As per claim 18, Easter as modified discloses the device as in claim 17. Easter further discloses wherein said memory location includes non-volatile memory (Easter: column 4 lines 57-65).

28. As per claim 19, Easter as modified discloses the device as in claim 18. Easter further discloses wherein said value stored in said memory location is defined during a manufacture of the monolithic semiconductor device (Easter: column 3 lines 54-64).

29. As per claim 21, Easter as modified discloses the device as in claim 19. Easter further discloses said value is defined using a laser etching technique (Easter: column 6 lines 5-13).

30. As per claim 22, Easter as modified discloses the device as in claim 17. Easter further discloses wherein said memory location includes volatile memory (Easter: column 4 lines 57-65).

31. As per claim 24, Easter as modified discloses the device as in claim 17. Easter further discloses wherein sad memory location is located in a specific location of the monolithic semiconductor device (Easter: figure 2).

32. As per claim 25, Easter as modified discloses the device as in claim 17. Easter further discloses wherein said value includes second encryption key (Easter: figure 5 and column 8 lines 18-26).

33. As per claim 26, Easter as modified discloses the device as in claim 25. Easter further discloses wherein said memory location is to store a plurality of encryption keys (Easter: figure 2 and column 4 lines 50-65).

34. As per claim 27, Easter as modified discloses the device as in claim 25. Easter further discloses wherein first encryption engine is to use a portion of the first encryption key to perform an encryption function (Easter: figure 5 and column 8 lines 18-40: the fuse array contains private key).

35. As per claim 28, Easter as modified discloses the device as in claim 25. Easter as modified further discloses wherein the first encryption key includes a symmetrical encryption key, and wherein said first encryption engine is an asymmetrical encryption engine and said second encryption engine is a symmetrical encryption engine (Easter: figure 5 and column 8 lines 18-26; Van Oorschot: column 5 lines 39-59).

36. As per claim 29, Easter as modified discloses the device as in claim 28. Easter as modified further discloses wherein said first encryption engine is to provide a symmetrical encryption key to said second encryption engine, and wherein said second encryption key is to perform an encryption function using the symmetrical encryption key (Van Oorschot: column 5 lines 39-59).

37. As per claim 30, Easter as modified discloses the device as in claim 17. Easter as modified further discloses wherein said isolation portion includes a fuse coupled between

the input of said external port and the output of said memory location (Pitts: Pitts: [0011]: the fuse element and figure 1: 104).

38. As per claim 31, Easter as modified discloses the device as in claim 17. Easter as modified further discloses the device comprising: at least one silicon die pad having an input coupled to the output of said memory location to provide a temporary access to said memory location (Easter: figure 2 and column 4 lines 50-65).

39. As per claim 32, Easter as modified discloses the monolithic semiconductor device as in claim 1. Easter further discloses the device comprising an unique ID register coupled to the input of said encryption engine to store an unique ID (Easter: column 5 lines 27-36 and figure 3).

40. As per claim 37, Easter discloses the method as in claim 33. Easter does not explicitly disclose the method including the steps of: accessing externally the data from the memory location; and isolating the memory location from subsequent external access. However, Pitts discloses an isolation fuse element that enforces one time programming of the memory (Pitts: [0011]: the fuse element and figure 1:104). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to include a fuse element in the semiconductor device because semiconductor device with fuse is well known in the art. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of

Pitts within the system of Easter because it prevents external access to the memory location after data has been successfully stored into secure memory array.

41. As per claim 38, Easter as modified discloses the method as in claim 37. Easter as modified further discloses the step of accessing externally includes verifying a value of the data (Pitts: [0011]: allow loading and testing of the secure memory array).

42. As per claim 39, Easter as modified discloses the method as in claim 37. Easter as modified further discloses the step of accessing externally includes defining a value of the data (Pitts: [0011]).

43. As per claim 40, Easter as modified discloses the method as in claim 37. Easter as modified further discloses the step of isolating includes blowing a fuse which allows external access to the memory location (Pitts: [0011]).

44. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Easter in view of Van Oorschot and further in view of Pitts and further in view of Loh.

45. As per claim 20, Easter as modified discloses the device as in claim 19. Easter as modified does not explicitly disclose wherein said value is defined using a lithographic technique. However, Loh discloses that limitation (Loh: [0003]:use of lithography). It would have been obvious to one having ordinary skill in the art to define value of the memory location using lithographic technique because lithography is one of the most

common technique for hardwired programming of the ROM on semiconductor. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Loh within the combination of Easter-Pitts because lithography is well known technique in semiconductor industry.

Response to Arguments

46. Applicant's arguments filed 11/16/05 have been fully considered but they are not persuasive.

Regarding applicant's remarks, applicant argues that the prior art of record fail to disclose an asymmetric encryption engine and a symmetric encryption engine and the asymmetrical encryption engine has an output port to provide a symmetrical encryption key based on a data value store in the memory location observable only to a monolithic semiconductor device. However, in figure 5 and column 8 lines 18-26 of the Easter reference, Easter clearly discloses that there are RSA and DES engines on the semiconductor device and the RSA engine provides output key to DES engine to perform symmetrical encryption. Therefore, applicant's argument is respectfully traversed.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100